Qualcomm® Inline Crypto Engine (UFS)

Version 3.1.0

FIPS 140-2 Non-Proprietary Security Policy

Version 1.3

2020-02-17

Prepared for:

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121

Prepared by:

atsec information security Corp.
9130 Jollyville Road, Suite 260
Austin, TX 78759

TABLE OF CONTENTS

1.Introduction

This document is the non-proprietary FIPS 140-2 Security Policy for the Qualcomm Inline Crypto Engine (UFS) cryptographic module. The version of this Qualcomm Inline Crypto Engine (UFS) is 3.1.0. This document contains a specification of the rules under which the Qualcomm Inline Crypto Engine (UFS) must operate and describes how this Qualcomm Inline Crypto Engine (UFS) meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 1 hardware cryptographic module.

1.1 Purpose of the Security Policy

There are three major reasons that a security policy is needed:

- It is required for FIPS 140-2 validation.
- It allows individuals and organizations to determine whether the Qualcomm Inline Crypto Engine (UFS), as implemented, satisfies the stated security policy.
- It describes the capabilities, protection, and access rights provided by the Qualcomm Inline Crypto Engine (UFS), allowing individuals and organizations to determine whether it will meet their security requirements.

2. Cryptographic Module Specification

2.1.Description of Module

The Qualcomm Inline Crypto Engine (UFS) is classified as a single chip hardware module for the purpose of FIPS 140-2 validation. It provides AES-XTS encryption and decryption of block storage devices. The logical cryptographic boundary is the Qualcomm Inline Crypto Engine (UFS) 3.1.0, which is a sub-chip hardware component contained within the Qualcomm® Snapdragon™ 845 SoC, the Snapdragon 855 SoC, the Snapdragon 865 Mobile Platform SoC, and the Qualcomm® Snapdragon™ 765 5G Mobile Platform SoC

The Qualcomm Inline Crypto Engine (UFS) implements AES-XTS encryption and decryption as defined in SP 800-38E. The underlying AES for AES-XTS is AES ECB compliant to FIPS 197.

The hardware sub-chip cryptographic module is specified in the following table:

Component	Type	Version Number
Qualcomm Inline Crypto Engine (UFS)	Hardware	3.1.0

Table 1: Components of the Hardware Cryptographic Module

The Qualcomm Inline Crypto Engine (UFS) has been tested on the following platforms:

- Snapdragon 845
- Snapdragon 855
- Snapdragon 865 Mobile Platform
- Snapdragon 765 5G Mobile Platform

The Qualcomm Inline Crypto Engine (UFS) is intended to meet the requirements of FIPS 140-2 at an overall Security Level 1. The table below shows the security level claimed for each of the eleven sections that comprise the validation:

FIPS 140-2 Sections	Security Level				
	N/A	1	2	3	4
Cryptographic Module Specification		X			
Cryptographic Module Ports and Interfaces		X			
Roles, Services and Authentication		X			
Finite State Model		X			
Physical Security		X			
Operational Environment	X				
Cryptographic Key Management		X			
EMI/EMC		X			
Self-Tests		X			
Design Assurance		X			
Mitigation of Other Attacks	X				

Table 2: Security Levels

2.2.Description of Approved Mode

The Qualcomm Inline Crypto Engine (UFS) supports only FIPS mode.

When the Qualcomm Inline Crypto Engine (UFS) is powered on, the power-up self-test is executed automatically without any operator intervention. The Qualcomm Inline Crypto Engine (UFS) enters FIPS mode automatically if the power-up self-test completes successfully.

If any of the self-tests fail during power-up, the Qualcomm Inline Crypto Engine (UFS) goes into Error state. All cryptographic services are prohibited while in error state. When an error state is entered, the Qualcomm Inline Crypto Engine (UFS) can be reset to reinitialize itself.

The status of the Qualcomm Inline Crypto Engine (UFS) can be determined by its availability. If the Qualcomm Inline Crypto Engine (UFS) is available, it has passed all self-tests. If it is unavailable, it is in the error state.

The Qualcomm Inline Crypto Engine (UFS) can be configured to operate in one of the following two settings where the settings can be changed prior to each service request:

- Full Disk Encryption (FDE) that performs an encryption of all write operations and a decryption of all read requests with one key.
- Per-File Encryption (PFE) that performs an encryption of one write operation and a decryption of one read operation with a key dedicated to this operation.

The Qualcomm Inline Crypto Engine (UFS) supports a key storage which allows either 2 hardware keys or up to 32 software selectable key contexts. Each context holds 2 AES keys needed for AES-XTS. One such context may be used for FDE or otherwise all 32 contexts may be used for PFE. When an encryption configuration is established, the chosen hardware key or the software selected context key is referenced and will be used for the operation by the Qualcomm Inline Crypto Engine (UFS).

The user of this Qualcomm Inline Crypto Engine (UFS) may also decide not to use the encryption/decryption services provided. Such a decision is not made within the boundary of the Qualcomm Inline Crypto Engine (UFS) itself. When the user chooses to disable any encryption for write requests and decryption for read requests, the Qualcomm Inline Crypto Engine (UFS) is simply not in use.

The Qualcomm Inline Crypto Engine (UFS) provides the following CAVP validated algorithm implementations:

Components	Algorithms	Standards	CAVS Certs #
Qualcomm Inline Crypto Engine (UFS)	AES ECB 128/256 encryption	FIPS 197	#4958,#C439,#C1418,#C1553
	AES ECB 128/256 decryption		#4957,#C440,#C1417,#C1552
	AES-XTS 128/256 encryption	SP-800-38E	#4958,#C439,#C1418,#C1553
	AES-XTS 128/256 decryption		#4957,#C440,#C1417,#C1552

Table 3: Approved Algorithms

2.3.Cryptographic Module Boundary

The physical boundary of the Qualcomm Inline Crypto Engine (UFS) is the physical boundary of the Snapdragon 845 SoC, the Snapdragon 855 SoC, the Snapdragon 865 Mobile Platform SoC, and the Snapdragon 765 5G Mobile Platform SoC that contains the sub-chip which implements the Qualcomm Inline Crypto Engine (UFS). Consequently, the embodiment of the Qualcomm Inline Crypto Engine (UFS) is a single-chip cryptographic module. The logical boundary is the Inline Crypto Engine sub-chip.

The following figure illustrates the various data, status and control paths through the physical and logical boundary of the Qualcomm Inline Crypto Engine (UFS).

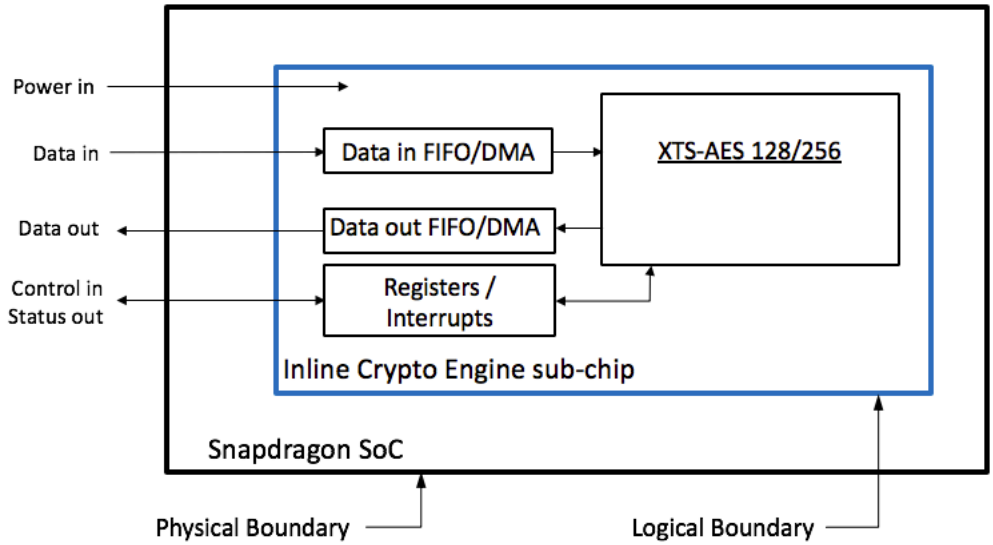

Figure 1: The Physical and Logical Boundary of Inline Crypto Engine (UFS)

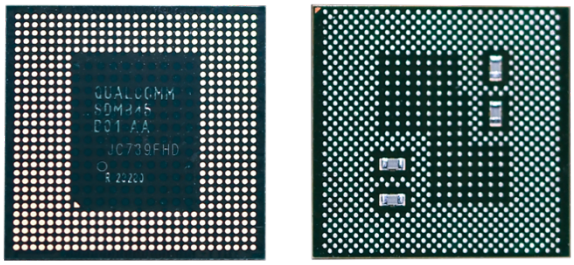

Figure 2: Snapdragon 845

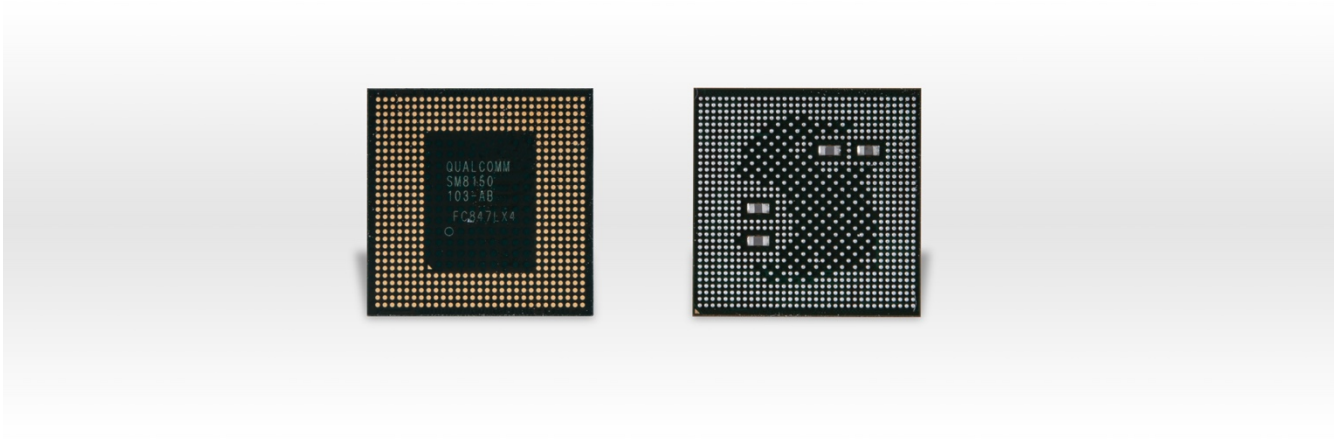

Figure 3: Snapdragon 855

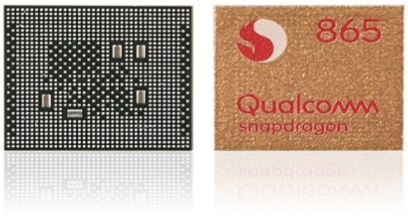

Figure 4: Snapdragon 865 Mobile Platform

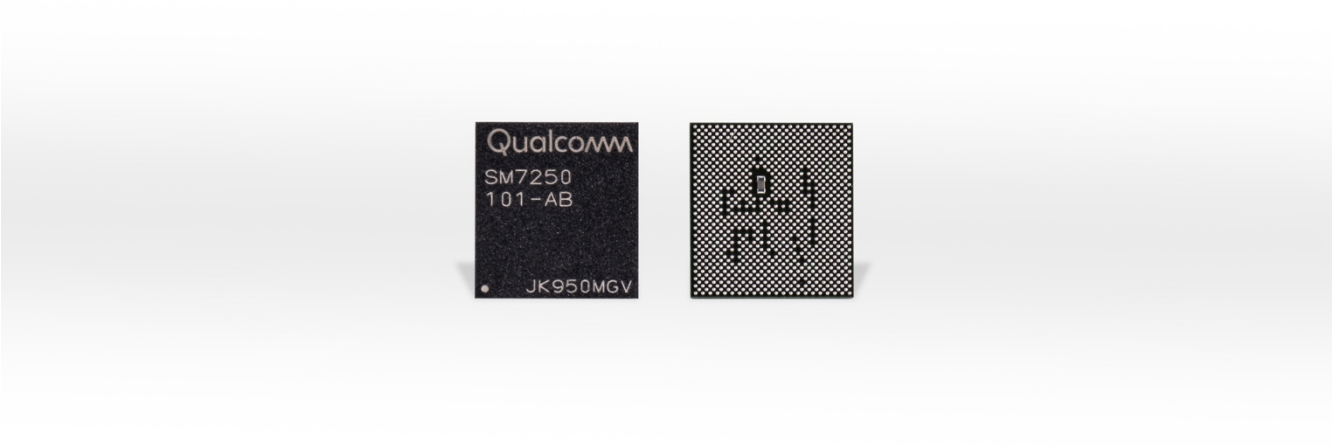

Figure 5: Snapdragon 765 5G Mobile Platform

3.Cryptographic Module Ports and Interfaces

FIPS Interface	Ports
Data Input	Data In FIFO/DMA
Data Output	Data Out FIFO/DMA
Control Input	Registers, Interrupts
Status Output	Registers, Interrupts
Power Input	Physical power connector

Table 4: Ports and Interfaces

4.Roles, Services and Authentication

4.1.Roles

Roles	Description
User	Perform general security services, including cryptographic operations; configuration of the Qualcomm Inline Crypto Engine (UFS) for FDE or PFE.
Crypto Officer (CO)	Configuring the key to be used for the cipher operation.

Table 5: Roles

The Qualcomm Inline Crypto Engine (UFS) meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both User and Crypto Officer roles. It does not allow concurrent operators.

The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the Qualcomm Inline Crypto Engine (UFS). No further authentication is required. The Crypto Officer is responsible to set the key for the cipher operation.

4.2.Services

The Qualcomm Inline Crypto Engine (UFS) provides AES-XTS-128/256 encryption and decryption. A user may choose whether or not to use the Qualcomm Inline Crypto Engine (UFS) for its designed services. Once the Qualcomm Inline Crypto Engine (UFS) is in use, it does not support a bypass capability to skip the requested encryption or decryption.

The following table describes the services available in FIPS-mode:

Services	Roles		CSP	Access (Read, Write, Execute)
	User	CO		
AES-XTS 128/256 encryption and decryption	✓		Two distinct AES keys	R, W
Self-Test (Self-Test is executed automatically when device is booted or restarted)	✓		N/A	N/A
Zeroization	✓		AES keys	R,W
Configuration of operational mode	✓		N/A	N/A
Status output	✓		N/A	N/A
Setting of encryption keys		✓	N/A	N/A

Table 6: Services available in FIPS-mode

Note: The methodology for setting the encryption keys is described in the ICE – Inline Crypto Engine Hardware Programming Guide.

4.3.Operator Authentication

There is no operator authentication; assumption of role is implicit by the used service(s).

4.4.Mechanism and Strength of Authentication

No authentication is required at security level 1; authentication is implicit by assumption of the role.

5.Physical Security

The Qualcomm Inline Crypto Engine (UFS) 3.1.0 is a sub-chip module implemented as part of the Snapdragon 845 SoC, the Snapdragon 855 SoC, the Snapdragon 865 Mobile Platform SoC, and the Snapdragon 765 5G Mobile Platform SoC which is the physical boundary of the sub-chip module. The Snapdragon 845 SoC, the Snapdragon 855 SoC, the Snapdragon 865 Mobile Platform SoC, and the Snapdragon 765 5G Mobile Platform SoC are single chips with a production grade enclosure and hence conforms to the Level 1 requirements for physical security.

6.Operational Environment

6.1.Applicability

The Qualcomm Inline Crypto Engine (UFS) is a single chip hardware module. The procurement, build and configuring procedure are controlled. Therefore, the operational environment is considered non-modifiable.

7.Cryptographic Key Management

7.1.Key and CSP List

The only keys/CSPs are the AES keys for AES-XTS encryption and decryption services. These keys are generated outside the Qualcomm Inline Crypto Engine (UFS) boundary and set up by the Crypto Officer in the registers of the Qualcomm Inline Crypto Engine (UFS).

The following table lists the key/CSP used by the Qualcomm Inline Crypto Engine (UFS):

Key/CSP	Generation	Storage	Zeroization
AES keys	N/A (Provided by caller, set by Crypto Officer)	Hardware memory (write-only by software)	Zeroized during cold boot of the Qualcomm Inline Crypto Engine (UFS)

Table 7: Keys and CSPs

7.2.Key/CSP Generation, Entry and Output

The Qualcomm Inline Crypto Engine (UFS) does not provide any key generation service or perform key generation for any of its Approved algorithms. The caller provides the keys for encryption and/or decryption. Keys are stored in hardware registers (write-only by software) by the Crypto Officer. Once the keys are written to the hardware registers, they are not readable from outside the Qualcomm Inline Crypto Engine (UFS).

The Qualcomm Inline Crypto Engine (UFS) does not provide any asymmetrical algorithms or key establishment methods.

7.3.Key/CSP Storage and Zeroization

As stated previously, the Qualcomm Inline Crypto Engine (UFS) stores all keys and CSPs internally. All keys and CSPs are stored in on-chip memory (RAM) and also in registers. The key storage memory is able to be read by the Qualcomm Inline Crypto Engine (UFS) itself and is write-only (not readable) from outside of the Qualcomm Inline Crypto Engine (UFS). When the Qualcomm Inline Crypto Engine (UFS) performs a cold boot, it will zeroize all CSPs contained within itself.

8.Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The Qualcomm Inline Crypto Engine (UFS) hardware component cannot be certified by the FCC as it is not a standalone device. It is a sub-chip embedded in the Snapdragon 845 SoC, the Snapdragon 855 SoC, the Snapdragon 865 Mobile Platform SoC, and the Snapdragon 765 5G Mobile Platform SoC which are also not a standalone device, but rather intended to be used within a COTS device which would undergo standard FCC certification for EMI/EMC.

According to 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, the Qualcomm Inline Crypto Engine (UFS) is not subject to EMI/EMC regulations because it is a subassembly that is sold to an equipment manufacturer for further fabrication. That manufacturer is responsible for obtaining the necessary authorization for the equipment within which the Qualcomm Inline Crypto Engine (UFS) embedded prior to further marketing to a vendor or to a user.

9.Power-Up Tests

Power-Up tests consist of known-answer tests (KAT) of algorithm implementations. The power-up self-tests are automatically performed without any operator intervention during power-up of the Qualcomm Inline Crypto Engine (UFS). If any of the power-up self-tests fails, the Qualcomm Inline Crypto Engine (UFS) will enter the error state. Data output is prohibited and no further cryptographic operation is allowed while in the error state. FIPS 140-2 explicitly allows a provision that the on-demand test can be fulfilled with a power cycle of the Qualcomm Inline Crypto Engine (UFS). Hence, a power cycle and its associated power-on self-test is the methodology used to perform the "on-demand" tests.

The power-up self-tests are also performed when a reset event is received. If any of the tests fail, the Qualcomm Inline Crypto Engine (UFS) will enter into an error state. The Qualcomm Inline Crypto Engine (UFS) cannot be used in this state. To recover from the error state, re-initialization is possible by successful execution of the power up tests, which can be triggered by either a power-off/power-on cycle or the receipt of a reset event.

The power-up self-tests are triggered immediately when a reset occurs. All needed tests are executed until completion. Once completed successfully, the control logic releases the Qualcomm Inline Crypto Engine (UFS) for external usage. If an error is detected during the tests, the control logic locks the Qualcomm Inline Crypto Engine (UFS) and prevents external usage. Once locked, the Qualcomm Inline Crypto Engine (UFS) will only respond to a reset which will cause it to re-execute the power up tests. If the error persists, the Qualcomm Inline Crypto Engine (UFS) will remain unavailable.

9.1.Cryptographic Algorithm Tests

Algorithm	Test
AES-256 Encryption (ECB)	KAT
AES-256 Decryption (ECB)	KAT

Table 8: Power-Up Cryptographic Algorithm Tests

9.2.Integrity Tests

Not applicable due to Qualcomm Inline Crypto Engine (UFS) is implemented in hardware and is non-modifiable

10.Design Assurance

10.1.Configuration Management

ClearCase, a version control system from IBM/Rational, is used to manage the revision control of the hardware code (Verilog code) and hardware documentation. The ClearCase version control system provides version control, workspace management, parallel development support and build auditing. The Verilog code is maintained within the ClearCase database used by Qualcomm Technologies, Inc.

11.Mitigation of Other Attacks

No other attacks are mitigated.

12. Glossary and Abbreviations

AES Advanced Encryption Specification

CMVP Cryptographic Module Validation Program

CSP Critical Security Parameter

FDE Full Disk Encryption

FIPS Federal Information Processing Standards Publication

KAT Known Answer Test

PFE Per File Encryption

SoC System on Chip

UFS Universal Flash Storage

13.References

[1] FIPS 140-2 Standard, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

[2] FIPS 140-2 Implementation Guidance, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

[3] FIPS 140-2 Derived Test Requirements, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

[4] FIPS 197 Advanced Encryption Standard, https://csrc.nist.gov/publications/fips

[5] FIPS 180-4 Secure Hash Standard, https://csrc.nist.gov/publications/fips

[6] SP 800-38E Recommendation for Block Cipher Modes of Operation: The AES-XTS Mode for Confidentiality on Storage Devices, https://csrc.nist.gov/publications/sp800